§170.315(h)(2) Direct Project, Edge Protocol, and XDR/XDM

2015 Edition CCGs

Version 1.6 Updated on 06-15-2020

Revision History

Version #	Description of Change	Version Date
1.0	Initial Publication	10-30-2015
1.1	Removed email protocol clarification that's not applicable for 2015 Edition certification. Added update reference for Delivery Notification in Direct. Added clarification on SMTP and XDR standards for HISP getting certified to (h)(2).	03-24-2016
1.2	Added clarification to note that certification to this criterion is the only option for "transport-only" focused Health Information Services Providers (HISPs), but certification would also allow the HISP technology to electronically exchange with any health IT certified to § 170.315(b)(1) and may be used to meet the 2015 Edition Base EHR definition with any other health IT certified to § 170.315(b)(1) without the need for joint certification.	07-06-2016
1.3		10-07-2016

	Added HISP guidance in regards to sending dispatched MDNs in production.	
1.4	Added definition of a secure network. Clarification of the cipher suite requirements due to updated standards.	07-07-2017
1.5	Revised the location of the Edge Testing Tool training videos in the section “applies to entire criterion". Clarified that Direct, the Edge protocols (SMTP & XDR) and XDM processing are required by this criterion, consistent with interpretative guidance provided in the 2015 Edition final rule in the section “applies to entire criterion”.	11-29-2017
1.6	Updated the Security requirements per 21st Century Cures Act.	06-15-2020

Regulation Text

Regulation Text

§170.315 (h)(2) *Direct Project, Edge Protocol, and XDR/XDM—*

(i) Able to send and receive health information in accordance with:
(A) The standard specified in §170.202(a)(2), including formatted only as a “wrapped” message;
(B) The standard specified in §170.202(b), including support for both limited and full XDS metadata profiles; and
(C) Both edge protocol methods specified by the standard in §170.202(d).

(ii) *Delivery Notification in Direct.* Able to send and receive health information in accordance with the standard specified in §170.202(e)(1).

Standard(s) Referenced

Paragraph (h)(2)(i)(A)

§ 170.202(a)(2) Direct Project: ONC Applicability Statement for Secure Health Transport, Version 1.2, August 2015

Paragraph (h)(2)(i)(B)

§ 170.202(b) ONC XDR and XDM for Direct Messaging Specification

Paragraph (h)(2)(i)(C)

§ 170.202(d) ONC Implementation Guide for Direct Edge Protocols, Version 1.1, June 25, 2014

Paragraph (h)(2)(ii)

§ 170.202(e)(1) Delivery Notification - Implementation Guide for Delivery Notification in Direct v1.0

Certification Companion Guide: Direct Project, Edge Protocol, and XDR/XDM

This Certification Companion Guide (CCG) is an informative document designed to assist with health IT product development. The CCG is not a substitute for the 2015 Edition final regulation. It extracts key portions of the rule's preamble and includes subsequent clarifying interpretations. To access the full context of regulatory intent please consult the 2015 Edition final rule or other included regulatory reference. The CCG is for public use and should not be sold or redistributed.

Link to Final Rule Preamble
Link to Correction Notice Preamble

Edition Comparision	Gap Certification Eligible	Base EHR Definition	In Scope for CEHRT Definition
Revised	No	Included	Yes

Certification Requirements

Privacy and Security: This certification criterion was adopted at § 170.315(h)(2). As a result, an ONC-ACB must ensure that a product presented for certification to a § 170.315(h) "paragraph (h)" criterion includes the privacy and security criteria (adopted in § 170.315(d)) within the overall scope of the certificate issued to the product.

- The privacy and security criteria (adopted in § 170.315(d)) do not need to be explicitly tested with this specific paragraph (h) criterion unless it is the only criterion for which certification is requested.
- As a general rule, a product presented for certification only needs to be tested once to each applicable privacy and security criterion (adopted in § 170.315(d)) so long as the health IT developer attests that such privacy and security capabilities apply to the full scope of capabilities included in the requested certification. However, exceptions exist for § 170.315(e)(1) "VDT" and (e)(2) "secure messaging," which are explicitly stated.

- § 170.315(d)(2)(i)(C) is not required if the scope of the Health IT Module does not have end-user device encryption features.

Table for Privacy and Security

- If choosing Approach 1:
  - Authentication, access control, and authorization (§ 170.315(d)(1))
  - Auditable events and tamper-resistance (§ 170.315(d)(2))
  - Audit reports (§ 170.315(d)(3))
  - Encrypt Authentication Credentials (§ 170.315(d)(12))
  - Multi-factor Authentication (MFA) (§ 170.315(d)(13))
- If choosing Approach 2:
  - For each applicable P&S certification criterion not certified for approach 1, the health IT developer may certify using system documentation which is sufficiently detailed to enable integration such that the Health IT Module has implemented service interfaces the Health IT Module to access external services necessary to meet the requirements of the P&S certification criterion. Please see the *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program* Final Rule at 85 FR 25642 for additional clarification.

Design and Performance: The following design and performance certification criteria (adopted in § 170.315(g)) must also be certified in order for the product to be certified.

- When a single quality management system (QMS) is used, the QMS only needs to be identified once. Otherwise, the QMS' need to be identified for every capability to which it was applied.
- When a single accessibility-centered design standard is used, the standard only needs to be identified once. Otherwise, the accessibility-centered design standards need to be identified for every capability to which they were applied; or, alternatively the developer must state that no accessibility-centered design was used.

Table for Design and Performance

- Quality management system (§ 170.315(g)(4))
- Accessibility-centered design (§ 170.315(g)(5))

Technical Explanations and Clarifications

Applies to entire criterion

Clarifications:

- In order to meet the Base EHR Definition, a provider would need to possess technology that has been certified to either this criterion at § 170.315(h)(2) or the "Direct Project" criterion at § 170.315(h)(1).
- Several training/demo videos of the Edge Testing Tool used for the testing and certification of health IT are available on GitHub.
  - Please address any ETT technical questions through the ETT Google Group: https://groups.google.com/forum/?hl=en#!forum/edge-test-tool
- This certification criterion uses the Applicability Statement for Secure Health Transport, Version 1.2 standard. This new version of the specification includes updates that improve interoperability

through the clarification of requirements that have been subject to varying interpretations, particularly requirements around message delivery notifications. This version also clarifies pertinent requirements in the standards underlying the Applicability Statement for Secure Health Transport. Refer to the standard for more details about the improvements it includes. [see also 80 FR 62679]
- Testing for this criterion will require the processing of invalid test cases that frequently occur in real-world situations so that Security/Trust Agents (STAs) can demonstrate error handling abilities, including handling XDM packages and message disposition.
- Direct, the Edge protocols (SMTP, XDR) and XDM processing are the required standards for health IT certifying to (h)(2). IMAP and POP3 are optional SMTP standards. [see also 80 FR 62680]
- Certification to this criterion is the only option for "transport-only" focused Health Information Services Providers (HISPs). However, HISP technology certified to this criterion would be able to electronically exchange with any health IT certified to § 170.315(b)(1). Further, HISP technology certified to this criterion may also be used to meet the 2015 Edition Base EHR definition with any other health IT certified to § 170.315(b)(1) without the need for joint certification of the products.
- Consistent with the Implementation Guide for Delivery Notification in Direct, ONC's policy intent is that the receiving HISP must provide delivery notification messages either when it is also the sending HISP, or when it is specifically requested to do so by the sending HISP. A HISP is not compelled to request delivery notifications, but a certified HISP is required to produce them if requested.
- A secure network is generally recognized as one where all of the nodes (endpoints) are known, uniquely identified, access controlled, with strong end-to-end encryption. For example, a virtual private network (VPN) or a network physically isolated from any other with specialized equipment using endpoint encryption.

Paragraph (h)(2)(i)

Technical outcome – The Health IT Module can electronically transmit (send and receive) health information to and from a third party using each of:

- Applicability Statement for Secure Health Transport, Version 1.2 (the "Direct Project" specification);
- The ONC XDR and XDM for Direct Messaging Specification, Version 1, including support for both limited and full XDS metadata profiles;
- And both of the protocols in the ONC Implementation Guide for Direct Edge Protocols, Version 1.1.

Clarifications:

- This criterion requires the three capabilities specified (Direct Project specification, Edge Protocol compliance, and XDR/XDM processing) because it must support interoperability and all potential certified exchange options. A provider could use an "independent" health information service provider (HISP) to meet the Base EHR definition. In such a case, the HISP would need to be certified to this criterion in order for the provider to use it to meet the Base EHR definition, which is part of the CEHRT definition under the EHR Incentive Programs. [see also 80 FR 62681]
- For developers implementing the ONC XDR/XDM for Direct Messaging Specification, when converting an SMTP message into XDR (with limited metadata), UUID URNs formatted as OIDs should be used for DocumentEntry.uniqueId, SubmissionSet.sourceId, and SubmissionSet.uniqueId We expect testing to this specification to reflect this clarification. [FAQ #31]
- Even though the IG for Edge Protocols requires support for XDS limited metadata, XDR/XDM supports capability to transform messages using full metadata wherever appropriate. Therefore, we require that a Health IT Module must support both the XDS Metadata profiles (Limited and Full), as specified in the underlying IHE specifications, to ensure that the transformation between messages packaged using XDR/XDM are done with as much appropriate metadata as possible. [see also 80 FR 62681]
- For certification to this criterion, we have made it a requirement to send and receive messages in only "wrapped" format even though the specification (IG) allows use of "unwrapped" messages. This requirement will further improve interoperability among Security/Trust Agents (STAs) while having minor development impact on health IT developers. [see also 80 FR 62679]

- The protocols listed in the Implementation Guide, section 1.3.1 explicitly list conformance to RFC 3501. The RFC, then originally published, mandated using the TLS_RSA_WITH_RC4_128_MD5 cipher suite within the TLS 1.0 bundle. RFC 3501 has had subsequent updates making the listed cipher suite obsolete and rescinded within the TLS 1.0 bundle. Current industry practice is to implement cipher suites that are compliant with TLS 1.1(shall), TLS 1.2 (should), and TLS 1.0 (may).

Paragraph (h)(2)(ii)

Technical outcome – The health IT can electronically transmit (send and receive) health information to a third party using Direct in accordance with the Implementation Guide (IG) for Delivery Notification in Direct, Version 1.0.

Clarifications:

- The Implementation Guide for Delivery Notification in Direct, Version 1.0, June 29, 2012 functionality supports interoperability and exchange, particularly for both sending and receiving parties, guidance enabling health information service providers (HISPs) to provide a high level of assurance to senders that a message has arrived at its destination, a necessary component to interoperability. The IG also outlines the various exception flows that result in compromised message delivery and the mitigation actions that should be taken by STAs to provide success and failure notifications to the sending system. [see also 80 FR 62729]
- For Delivery Notification in direct, the capability to send and receive health information must be in accordance with the standard specified in § 170.202(e)(1).

Content last reviewed on June 23, 2020